Risk Assessment - Approaches & Issues

A Panel Discussion

RSAC PTC Working Group

May 14th, 2002

Panelists

- Dr. Alan Bing – ICF Consulting
- Dr. Sherry Borener – U.S. DOT – Volpe Center
- Dr. Ted Giras – UVA Center for Safety-Critical Systems
- Dr. John Wreathall – The Wreathall Group

Panel Format

- Each participant will outline their approach and perspective on risk assessments
- Context will be guidelines offered in NPRM 49 CFR Part 209 et al
- Questions
  - RSAC Working Group Members
  - Panel members
- Summary / Wrap up

NPRM Refresher

- Risk Assessment - *means the process of determining, either quantitatively or qualitatively, the measure of risk associated with*
  (1) Use of the product under all intended operating conditions or
  (2) The previous condition."
- FRA envisions - that the risk assessment will identify the assigned risk classes for the system, assign a numerical expression for each safety integrity level, specify a target failure rate, and identify the standards upon which the assessment and calculations were made.
- The primary goal - of the risk assessment required by this proposed rule is to give an objective measure of the levels of safety risk involved for comparison purposes.

NPRM Refresher – continued

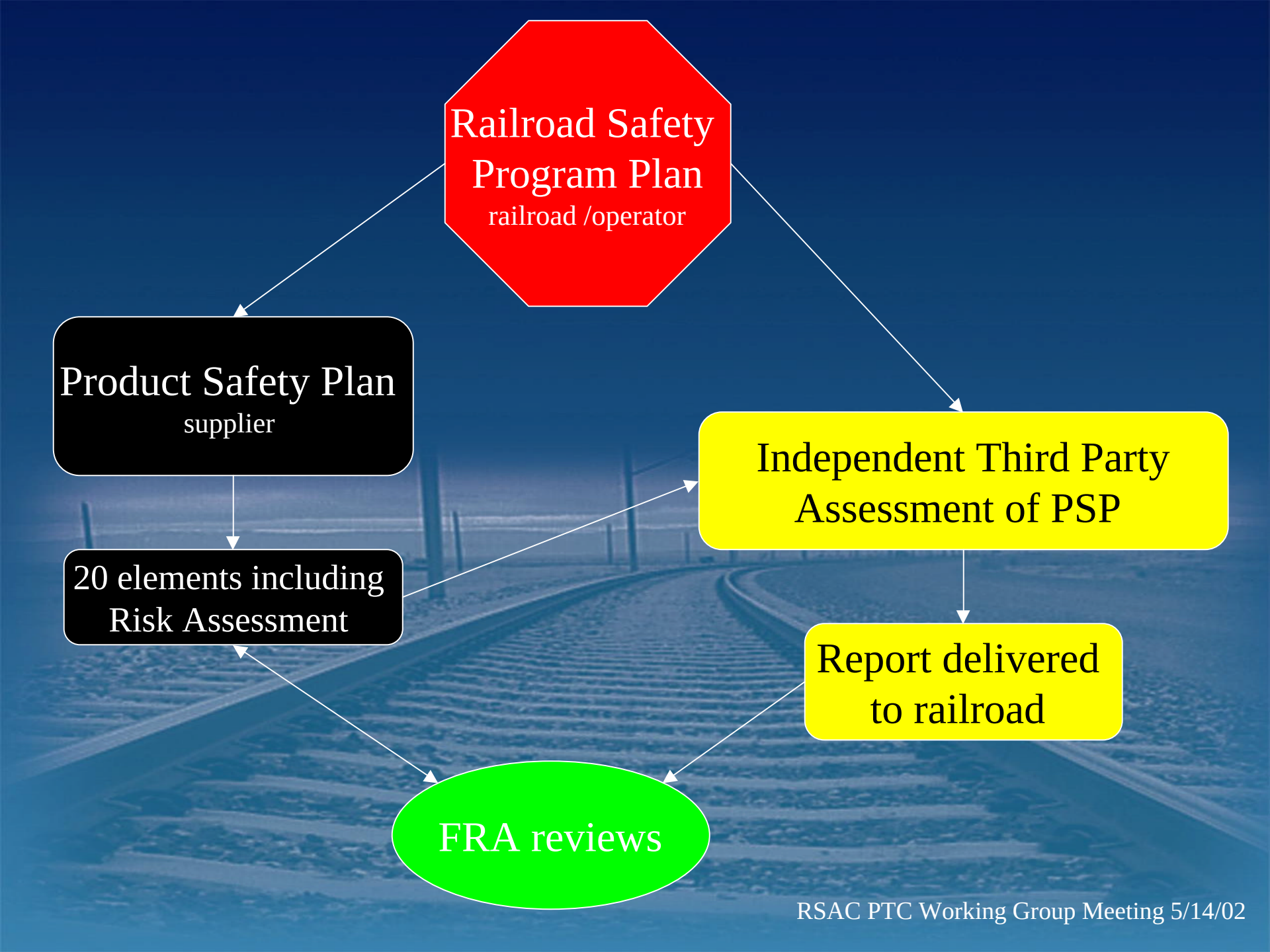
- The proposed rule - would allow both quantitative and qualitative risk assessment methods to be used, as well as combinations of the two. FRA expects that qualitative methods should be used only where appropriate, and only when accompanied by an explanation as to why the particular risk cannot be fairly quantified.
- FRA proposes - that risk assessment methods not meeting the guidelines of this proposed rule be allowed, so long as it could be demonstrated to the FRA Associate Administrator for Safety that the risk assessment method used is suitable in the context of the particular product.

NPRM Refresher – continued

- For all human-machine interface components/subsystems, FRA proposes appropriate MTTHE estimates be assigned.
- FRA feels it is important to verify that software assumptions are realistic and not overly optimistic.
- For the previous condition and for the life-cycle of the product, risk levels must be adjusted for exposure.

How it all fits together – elements of Part 236 h NPRM

- Product Safety Plan (PSP)
  - 20 requirements (product description, operation environment and concept, safety requirements and proposed architecture,, hazard log, **risk assessment**, hazard mitigation, safety assurance process and concepts, human factors analysis, training requirements, test procedures and equipment, applicability of subparts A-G, security requirements over life cycle, warning labels, post installation proof of continuity of safety, safety-critical assumptions and backup procedures, and proof of safety of pre-defined changes (must account for in the risk assessment).


Railroad Safety Program Plan
railroad /operator
Product Safety Plan
supplier
Independent Third Party Assessment of PSP
20 elements including Risk Assessment
Report delivered to railroad
FRA reviews